UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

PATRICK COLLINS, INC.
DBA ELEGANT ANGEL
8015 Deering Ave
Canoga Park, CA 91304

Plaintiff,

v.

DOES 1 – 67

Defendants.

Civil Action No. _____

I, Jon Nicolini, declare as follows:

1. I am the Chief Technology Officer of Copyright Enforcement Group, LLC ("CEG").

2. CEG's address is 8484 Wilshire Boulevard, Suite 220, Beverly Hills, California 90211.

3. CEG is in the business of discovering infringements, and arranging for the enforcement, of the copyrights of its clients. Plaintiff in this case is a client of CEG. Based on information provided to me, I state that Plaintiff is a motion picture creator and distributor, and the motion picture named in the Complaint (hereinafter the "Work") is among the motion pictures whose copyrights are the subject of the CEG's efforts.

4. Music and motion picture piracy (i.e., the unauthorized copying and/or distribution of songs and motion pictures) has been a problem since the advent of home audio and video devices. The problem continued with the introduction of home CD and DVD players. An article describing the problem when CDs and DVDs were a popular way to distribute audio and visual works can be found here:

http://www.thefreelibrary.com/DVD+piracy+in+the+U.S.+becomes+an+industry-a0103403775 (attached to this Declaration as **Exhibit B**)

Today, piracy has increased dramatically with the ability to store digital files of songs and motion pictures in the memory of home and/or laptop computers, as well as other devices such as iPads and iPhones. (In this Declaration, the term "computer" is, unless otherwise stated, meant to refer to any device or system that may store data and communicate on the Internet. Common examples of computers include, but are not limited to: desktop computers, laptop computers, tablet computers, smartphones, electronic readers, media players and even home entertainment systems.) Technology developments over the last several years allow people to distribute such files to each other over the Internet on peer-to-peer networks (sometimes called "P2P" networks) using file sharing software applications such as BitTorrent. Articles describing aspects of motion picture piracy, as well as piracy of games and books, over P2P networks could be found, at least until recently, at these web pages, among others:

http://www.forbes.com/2009/08/04/online-video-piracy-technology-e-gang-09-movies.html (attached to this Declaration as **Exhibit C**)

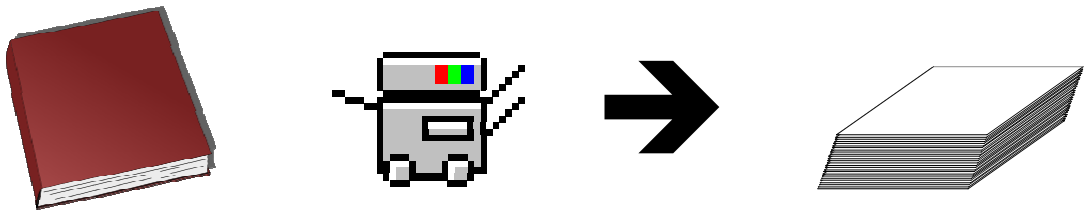
http://www.mpaa.org/resources/8aaaecf5-961e-4eda-8c21-9f4f53e08f19.pdf (attached to this Declaration as **Exhibit D**)

http://www.forbes.com/2008/09/12/spore-drm-piracy-tech-security-cx_ag_mji_0912spore.html (attached to this Declaration as **Exhibit E**)

http://reviews.cnet.com/8301-18438_7-20033437-82.html (attached to this Declaration as **Exhibit F**).

5. Before explaining how a P2P network, in particular a BitTorrent P2P network, works, I will describe a hypothetical "old school" example of cooperative copyright infringements. While this example is not 100% analogous to P2P infringements, it illustrates in an easy to understand manner how separate people, while committing a series of separate copyright infringements, can cooperate together to expedite the process of making unauthorized copies. A law student (let's call him or her the "first student") in a law school class of 100 students makes a copy of a casebook, for example Prosser, Wade, Schwartz, Kelly and Partlett's Cases and Materials on Torts, - 12th Edition ("Torts Casebook"). The first student figures that he or she will be lauded for making a copy of that very expensive book and making it available for

further copying by classmates. That first student made a significant investment of money purchasing the Torts Casebook, and spent considerable time in the page by page photocopying from the bound casebook to come up with 1,276 pages of a single-sided copy of the Torts Casebook:



However, what the first student ultimately wants, besides being a "hero" among certain of his/her classmates with respect to the Torts Casebook, is for other people in the class to do the same with respect to the Criminal Law Casebook, the Civil Procedure Casebook, and all the other books. The first student would be getting all books for the year for just the price of one book, while most students partaking in the scheme would be getting all books for free. In any event, the first student sends out a notice that there will be a book copying event in a certain room, in which stands a free photocopier, for anyone who wants to make a copy of the Torts Casebook. The first student would require, however, that anyone (referred to as a "subsequent student") who wants to leave the room with a copy must leave a copy behind for anyone else who comes to the room seeking to make another copy. If the copier is a 60 pages per minute copier, each student making a copy of the book from the first student's unauthorized copy would still have to invest just over 21 minutes of time to make a copy, but at over $150 for a new authorized copy of the book or $65 for a used authorized copy (according to Amazon.com on March 6, 2012), the money saved by the subsequent student's engaging in making an unauthorized copy could easily justify the time spent. The first student has saved the subsequent student a significant amount of time by making a unbound, single-sided copy available as opposed to the authorized bound copy. The time required for each infringement could be significantly decreased if there are multiple photocopiers available and the pages of the first student's unauthorized copy are divided among them. For example, if four photocopiers are available, the first student's notice could read and look like this,

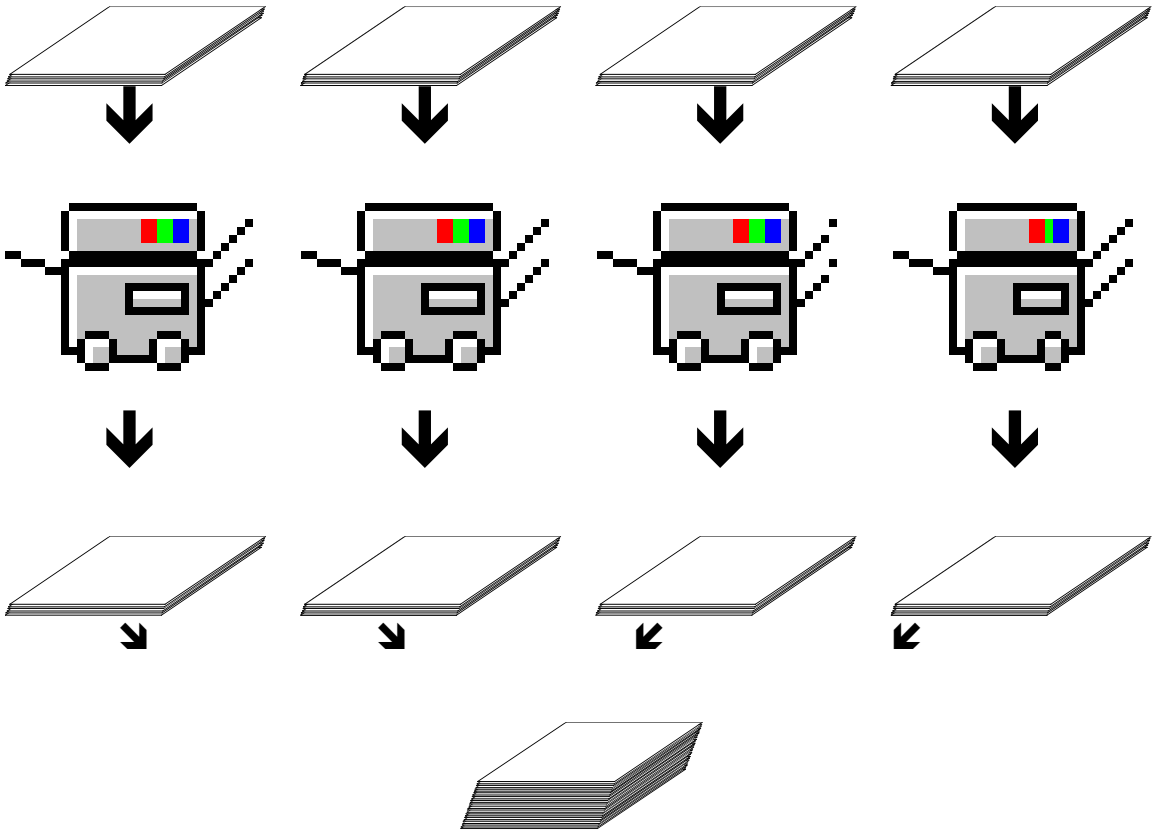
```
A copy of the Torts Casebook,

Prosser, Wade, Schwartz, Kelly and
Partlett's Cases and Materials on
Torts, - 12th Ed.
is available for you to copy in room
123.

The first 319 pages are in photocopier
1
Pages 320-638 are in photocopier 2.
Pages 639-957 are in photocopier 3.
Pages 958-1276 in photocopier 4.

Run a copy of each block of pages, take
the new copy
for yourself, and leave the 'original'
in each photocopier.
```

The first student might post the notice in the torts classroom, and in any or every room in which the first student would expect classmates to see such a notice. A subsequent student just starts the photocopiers and less than 6 minutes later scoops up from the photocopiers' output trays a complete copy (1276 pages) of the Torts Casebook. The next student comes in and puts the four sections of the first student's unauthorized copy of the Torts Casebook back into the respective input trays of the four photocopiers, and repeats the process. As long as the students cooperate by each making a new unauthorized copy and not merely grabbing the copy that is there, all 99 of the first student's classmates could have a copy of the Torts Casebook in just under 10 hours, with each student's time investment being less than 6 minutes.



The photocopy machines are of course mere tools, being useful for a student to innocently make copies of a moot court brief as well for the student to non-innocently make unauthorized copies of the works created by others. Of course, that "old school" type of copying was and is relatively rare because there was, and is, a significant and obvious risk of being easily caught.

6. With that "old school" example having been described above, I will now describe how BitTorrent peer-to-peer copying works. As noted above, BitTorrent peer-to-peer copying is somewhat similar to the "old school" example, and relies even more on cooperation. It should be kept in mind that just as photocopying a book may not be unlawful–for example, the book may be out of copyright. Merely using BitTorrent to copy a file is not unlawful if the file being copied is a digital file of a public domain work.

7. Neither of the two major operating systems for personal computers (i.e., those developed by Microsoft Corporation and Apple, Inc.) nor any of the four most used web browsers, namely, Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apple

Safari, which are used by well over 90% of users in the United States, include native functionality for peer-to-peer file sharing over the Internet. Regarding the relative popularity of browsers, see the following articles that could be found, at least until recently, at these web pages, among others, on the Internet:

http://gs.statcounter.com/#browser-US-monthly-201103-201202-bar (attached to this Declaration as **Exhibit G**)

http://www.statowl.com/web_browser_market_share.php?1=1&timeframe=last_3&interval=month&chart_id=4&fltr_br=&fltr_os=&fltr_se=&fltr_cn=&timeframe=last_12 (attached to this Declaration as **Exhibit H**).

Other than Microsoft Internet Explorer and Apple Safari, all other browsers must be intentionally installed. Therefore, the original "seeder" and each of the other members of the "swarm" (i.e., each of the "peers") must have separately installed on their respective computers special software that allows peer-to-peer sharing of files by way of the Internet. (The terms of art, "seeder," "peer," "leechers," and "swarm," will be described below.) The most popular type of peer-to-peer file sharing utilizes the BitTorrent protocol, in connection with which the seeder and members of the swarm use software (or applications) known as "BitTorrent clients." (In this context, the word "client" means a computer application that works in a BitTorrent environment.) Among the most popular BitTorrent clients are Vuze (formerly Azureus), µTorrent, Transmission and BitTorrent 7, although many others are used as well. In peer-to-peer network sharing, a "swarm" is a group of seeds and peers sharing a digital file through the same torrent file. A "peer" is one of the computers in a swarm sharing the digital file. A "seed" is a complete copy of the digital file of a work being made available for download. A "seeder" is either the computer on which the digital file was originally made available to a swarm, or a peer that has completed downloading the digital file and is making it available to others. Often, the people operating the computers are referred to as seeders, or seeds or peers as appropriate. In addition, "peers" are sometimes referred to as "leechers" (i.e. a peer that downloads more than it uploads), though the BitTorrent system is designed for every peer to become a partial seeder once that peer has received even one piece of the desired digital file. In any event, the seeder and every other

member of the swarm (i.e., peer) must intentionally install a BitTorrent client (i.e., software application) onto his/her computer before that computer can be used to join a BitTorrent P2P file sharing network.

8. P2P networks distribute infringing copies of motion pictures (and works in other forms such as music, games and books) with file sharing software such as BitTorrent as follows: The process begins with a person who decides that a particular work should be available for free to his/her fellow Internet users. After obtaining a digital file of the work or taking the work and making a digital file copy of it, that person uses a BitTorrent client to create what is called a "torrent file." A torrent file is uniquely associated with the digital file of the work (sometimes referred to as the "content file"). That person, who I will refer to as "the initial seeder," then accesses the Internet through an Internet Service Provider ("ISP") and intentionally makes the content file of the work available on the Internet to the public from his/her computer. That content file on the initial seeder's computer is often referred to as the first or initial "seed."

9. As indicated above, there is a one-to-one relationship between the content file and the torrent file. The torrent file, among other things, points to the content file. While the content file is very large, the torrent file is very small. The torrent file describes the content file that is being distributed, what pieces, often referred to as "blocks" or "chunks," into which the content file is divided, and other information needed for distribution of the content file. Typically, the title of the torrent file would include the name of the work included in the content file. The initial seeder would make his/her torrent file available on one or more websites. Alternatively, instead of uploading the torrent file to one or more websites, an initial seeder could make a link, often referred to in the field as a “magnet link,” available on one or more websites. The magnet link is a relatively new medium by which peers can access torrents. Its popularity is due to its not requiring the hosting of any files on a continuously available website. The magnet link is a uniform reference indicator (“URI”) scheme similar to a uniform reference locator (“URL”) that, when clicked, allows the aforementioned torrent file to be downloaded from other peers (at first the initial seeder) connected to the swarm as opposed to an individual web server. In either event, for a piece (or block) of a content file to be copied by one peer

from another member of the swarm that is acting as a seeder (e.g., because that other member has at least one block of the content file), both computers must have the same torrent file. The torrent file includes other data such as the separate hashes for each of the pieces into which the content file is divided for BitTorrent P2P distribution. (A "hash" is an alphanumeric string of characters mathematically derived from the characteristics of a file.) With the block-hash data, the computer doing the downloading, after it receives a block, does, through the BitTorrent client on its computer, a mathematical analysis of the downloaded block to confirm that that block has the hash that it should. That guarantees that only correct pieces of the content file are copied from one computer to another.

10. By way of a broad analogy, the "content file" would be similar to the 1,276 page unauthorized copy of the Torts Casebook made by the first student in the "old school example" given above. The first student would be similar to the "initial seeder," the "blocks" into which the content file is divided for distribution would be similar to the sets of pages into which the 1,276 pages were divided, the "torrent file" would be similar to the notice posted by the first student, the BitTorrent P2P network "swarm" (i.e., all the computers that have joined the swarm) would be analogous to the room with the photocopy machines in it, and the subsequent students would be similar to "peers."

11. With the title of the work being at least part of the torrent file's title, Internet users looking for a work will likely find the torrent file. In fact, people looking to obtain a copy for free could actually search online for the title of the work plus the word "torrent." Persons seeking to download such a work also access the Internet through an ISP (which may or may not be the same ISP as used by the initial seeder) and seek out the work on a P2P network. When such a person finds it, he/she downloads the subject torrent file. Then, opening that torrent file with his/her BitTorrent client, he/she can have his/her computer join the "swarm," that is, join the group of people exchanging the work among themselves. In turn, as each peer receives portions of the seed, most often that peer makes those portions available to other peers in the swarm. Therefore, each peer in the swarm is at least copying and is usually also distributing pieces of the work at the same time.

12. Any BitTorrent client may be used to join a swarm. As more peers join a swarm at any one instant, they obtain the content at even greater speeds because of the increasing number of peers simultaneously offering the content as seeders (or at least partial seeders) themselves for distribution of the work. In this regard, a swarm that starts with an initial seed may at any later time have tens, hundreds, or thousands of partial and complete seeds. Seeds and peers may enter, leave and re-enter a swarm at any time. As time goes on, the size of the swarm varies, yet it may endure for a long period, with some swarms enduring for 6 months to well over a year depending on the popularity of a particular work. CEG is monitoring torrent swarms which remain active today even after the original upload of a torrent file in 2009. As a result, the initial seed file becomes duplicated multiple times by multiple parties, with a potentially exponential increase in the number of copies of any work. With respect to any particular swarm, the hash (an alphanumeric representation of a file) of a torrent file remains the same.

13. The premise of BitTorrent sharing is well known, and is stated on the Bittorrent.com website, at least until recently here,

http://www.bittorrent.com/help/guides/beginners-guide (attached to this Declaration as **Exhibit I**)

as follows:

> "BitTorrent is a protocol (a set of rules and description of how to do things) allowing you to download files quickly by allowing people downloading the file to upload (distribute) parts of it at the same time. BitTorrent is often used for distribution of very large files, very popular files and files available for free, as it is a lot cheaper, faster and more efficient to distribute files using BitTorrent than a regular download."

14. As can be seen here,

http://www.bittorrent.com/help/faq/concepts (attached to this Declaration as **Exhibit J**)

my description given above is consistent with BitTorrent, Inc.'s own description.

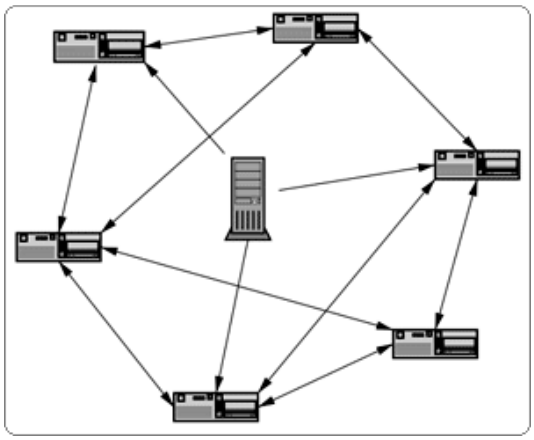
15. An explanation of the BitTorrent system and process can be found at a webpage found at:

http://bittorrent.org/introduction.html (attached to this Declaration as **Exhibit K**)

That web page is linked to from BitTorrent, Inc.'s own website. This is the explanation they provide:

> "The key to scaleable and robust distribution is cooperation. With BitTorrent, those who get your file tap into their upload capacity to give the file to others at the same time. Those that provide the most to others get the best treatment in return. ('Give and ye shall receive!')
>
> "Cooperative distribution can grow almost without limit, because each new participant brings not only demand, but also supply. Instead of a vicious cycle, popularity creates a virtuous circle. And because each new participant brings new resources to the distribution, you get limitless scalability for a nearly fixed cost.
>
> "BitTorrent is not just a concept, but has an easy-to-use implementation capable of swarming downloads across unreliable networks."

The web page also provides this diagram of the initial seeder and peers with accompanying wording:



The BitTorrent Solution:▫
Users cooperate in the distribution

Note that in P2P networks, the copying may continue even after the initial seeder has gone completely offline because of the replication perpetually occurring in the swarm.

16. Each user of a computer that has a particular torrent file on his/her computer and has joined a swarm related to that torrent file, has voluntarily caused his/her computer to "shake hands" with other members of the swarm to either copy the content file associated with the torrent file or to enable another member of the swarm to copy a portion of the content file from his/her computer, or both. This is a deliberate act. Unlike stumbling onto, for example, a youtube.com web page that automatically plays a video, with the Internet user merely watching the video on that web page, anyone who downloads a movie over a P2P network has taken several intentional steps while connected to the Internet to download (that is, make a copy of) the movie. These voluntary steps include: (i) making sure that the user's computer includes a BitTorrent client (an application as described above), (ii) finding a torrent file, or a magnet link to a torrent file, on the Internet associated with the desired content, (iii) actually downloading that torrent file on to the user's computer, by clicking on the torrent file link or on the magnet link to the torrent file, and (iv) starting the BitTorrent client, (v) using the BitTorrent, locating and opening the torrent file on the computer, and (vii) clicking on "OK" or a similar button in the BitTorrent client to start the downloading of the content file. Sometimes, steps (iv) and (v) are reversed. That is, the user finds the torrent file on his/her computer, clicks on it and his/her

computer launches his/her BitTorrent client with the torrent file opened in it. When a magnet link is used, steps (iii), (iv) and (v) appear to be combined into a single step. That is, upon the user's clicking on a magnet link, the torrent file is downloaded to his/her computer and his/her BitTorrent client is launched with the torrent file opened in it. In any event, the user still must, even after clicking on the magnet link, purposely click on the "OK" button in the BitTorrent client to begin downloading the content file. At that point, the torrent file makes the computer a part of the swarm, with the computer copying from and often distributing the content file to others. Continuing in this regard, even after the person has downloaded the desired movie, his/her computer will, unless set otherwise, continue allowing others to copy from it.

17. When an unauthorized copy of a copyrighted work is the content file in question, each peer (i.e. member of a swarm) in a P2P network sharing that unauthorized copy has acted and acts in cooperation with the other peers by providing an infringing reproduction of at least a portion of a copyrighted work. This is done in anticipation of other peers doing likewise with respect to that work and/or other works. The act of joining a P2P network is, as noted above, intentional, requiring the selection by a peer of URLs, links, and/or files, and then the clicking of an "OK" button to do so.

18. Depending on the particular P2P network involved, at any one time any number of people, from one or two to tens of thousands, unlawfully use the P2P network to upload (i.e. distribute), or download (i.e. copy or replicate), copyrighted material. To the extent that persons using a P2P network identify themselves, they use "user names" or "network names" which typically are nicknames that do not disclose the true identity of the user, and do not indicate the residence or business address of the user. So, while, as I explain below, we can detect infringements, we can only identify the infringers by their Internet Protocol address ("IP address") and the time that the infringement is detected by us. Note that while we detect an infringement at a particular instant, the infringer may have been infringing at other times as well.

19. The use of P2P networks, such as those accessed with BitTorrent software, to make unauthorized copies of motion pictures has become such common knowledge that it is casually mentioned in newspaper articles. For example, in the article titled "The Glut of Shows

Unwatched" published on the New York Times website, and which at least until recently could be seen at this web page:

> http://www.nytimes.com/2010/09/06/business/media/06carr.html (attached to this Declaration as **Exhibit L**),

there is this statement by the article's author who was describing his efforts to find a television show he had missed:

> "Starting to feel desperate, I thought for a moment about hopping on the laptop and searching BitTorrent for an illegal copy, but given that I make a living creating original content for a large media company, stealing from another one did not seem like a good idea."

20. Plaintiff and other similarly situated companies contract with CEG to have CEG determine whether or not copies of their works are being distributed on the Internet without their permission, and to identify infringers. Plaintiff does not authorize distribution of its motion pictures on P2P networks. Further in this regard, CEG is in no way involved in creating the torrent file used in any swarm, nor in making any content file available for downloading by members of a swarm except to the extent that CEG has obtained any blocks of a content file from other peers or seeds during a monitoring session.

21. CEG utilizes a system of software components ("the System") conceptualized, developed, and maintained by me in order to collect data about unauthorized distribution of copies of copyrighted works on P2P networks.

22. The System was designed for certain functions including, but not limited to: downloading substantial portions of content files from seeds and peers in a swarm, verifying data accuracy and accountability processes, confirming infringements, logging evidence, and the absolute prevention of false-positives. In fact, the System has multiple levels of error detection, and its architecture is conducive to preventing false-positives. Every unique suspect content file is visually verified by two people upon its inaugural acquisition.

23. The process as it relates to monitoring copyrighted works of CEG's clients begins as follows. When a copyrighted work is requested to be monitored, we use a web-based search

to find torrent files on the Internet that have the same title as the copyrighted work. As indicated above, a torrent file is a small file. Its file extension is ".torrent." A BitTorrent P2P network infringer will at some point have both the torrent file and at least a portion of the illegal copy file of the work (sometimes referred to herein as the "accused file") on the infringer's computer. In every case that a CEG client's motion picture is available on a P2P network, it is an unauthorized distribution of the motion picture.

24. Like any other person who wants to be a peer, we locate a torrent file relevant to a particular motion picture of one of our clients, download that torrent file to the System, and join the swarm associated with that torrent file on the Internet.

25. When a digital copy file with the same name as CEG's client's motion picture is found on a P2P network, CEG downloads a full copy of the suspect content file. The file is then forwarded to a two stage verification process. First, one person plays the downloaded file to visually confirm that the downloaded file is at least a portion of the client's motion picture. If that confirmation is made, then a second person independently plays the downloaded file for the same purpose. If both people confirm that a substantial portion of the motion picture in the suspect file is substantially the same as a corresponding portion of CEG's client's motion picture, then particular unique data (in particular, a "hash") relating to the torrent file associated with the suspect content file (now referred to in this Declaration as the "accused file") is noted by the System, and the System searches for additional computers on the P2P network that have, and are actively distributing, the accused file through that torrent file (hereinafter the "infringement enabling torrent file"). Note that any particular work may be the subject of copying by two or more different initial seeders. In such a case, the two torrent files would have different hashes from each other, and each would be the basis for a separate swarm. CEG tracks the swarms separately, and all Doe Defendants listed in any one case were members of the same, single swarm.

26. Users subscribe to the services of an ISP to gain access to the Internet. Each time a subscriber accesses the Internet, the ISP automatically allocates a unique IP address to the subscriber. An ISP generally records the times and dates that it assigns each IP address to a

subscriber and maintains for a period of time a record of such an assignment to a subscriber in logs maintained by the ISP. In addition, the ISP maintains records which typically include the name, one or more address, one or more telephone numbers, and one or more email addresses of the subscriber. P2P technology relies on the ability to identify the computers to and from which users can share files. The technology identifies those computers by the IP address from which the computer connects to the Internet. Taking advantage of this technology and the unique data associated with the torrent file having a one-to-one relationship with the file containing the unlawful copy of CEG's client's motion picture, CEG's System inspects file-sharing networks for computers that are distributing at least a substantial portion of a copy of a copyrighted work owned by Plaintiff. That is, CEG searches for computers that are active members of the swarm, uploading and downloading the accused file through use of the infringement enabling torrent file. When CEG finds such a computer, CEG downloads a portion of the copy of the accused file from the located computer using the infringement enabling torrent file. CEG's System also logs the following publicly accessible information relating to each computer from which CEG has downloaded a portion of the copy of the accused file:

(a) the time and date that CEG's System observed the infringer connected to the P2P network with respect to the infringer's computer's downloading and/or uploading the accused file to the Internet (hereinafter referred to as "Timestamp"),

(b) the IP address from which the infringer's computer was connected to the Internet at that time and date,

(c) the BitTorrent client used by the infringer and the port number used by the infringer’s BitTorrent client,

(d) the size of the accused file on the observed infringer's computer,

(e) the percent of the accused file downloaded by CEG from the infringer's computer,

(f) the hash of the torrent file that is associated with the accused file, and

(g) any relevant transfer errors.

To the extent that any relevant transfer errors do exist, the particular instance is removed from the System. To ensure the accuracy of the Timestamp, each of CEG's tracking servers has a Network Time Protocol daemon (i.e., program running in the background) deployed. This program maintains the System time in synchronization with time servers on the Internet. CEG has used this software since the inception of the System.

27. In addition, CEG uses available databases to record the name of the ISP having control of the IP address and available geolocation databases to record the United States state (and often the city) associated with that IP address. However, because of the partially anonymous nature of the P2P distribution system used by Defendants, the true names, street addresses, telephone numbers, and email addresses of Defendants are unknown to Plaintiff at this time.

28. As an additional check, CEG rejoins the swarm associated with the suspect torrent file and again downloads the entire unauthorized copy of the motion picture. This new download is viewed by a person to confirm that it is a copy of at least a substantial portion of the Plaintiff's motion picture. Thus, CEG has confirmed that each of the files downloaded by it from the Doe Defendants listed in **Exhibit A** attached to the Complaint filed in this case is a copy of at least a substantial portion of the copyrighted work listed in **Exhibit A**. All of this information is stored in database files on CEG's computers.

29. As indicated above, an Internet Protocol address (IP address) identifies the internet connection through which a computer accessed the Internet to commit the copyright infringement. The IP address utilized by P2P networks, and collected by CEG, is the public address, which is a globally unique address. If one knows a computer's public IP address, one can, using publicly available reverse-lookup databases on the Internet, identify the ISP used by that computer as well as the United States city and state in which the computer was located. Based on the information from such a database, CEG believes that computers associated with all the Doe Defendants listed in **Exhibit A** were used in infringements of Plaintiff's Work in the state in which the court listed in the caption above is located. However, the actual name and

address of the person subscribing to the ISP's service is neither publicly available, nor available to CEG.

30. With the Internet Protocol address and the date and time that the infringer's computer was accessing the Internet through the ISP, the ISP (be it AT&T, Verizon, Qwest, Comcast or any other ISP) can review its own subscriber logs to identify either (i) the names and addresses of the subscriber, or (ii) the intermediary ISP through which the person is ultimately subscribed to the main ISP. In turn, if the intermediary ISP is provided with the Internet Protocol address and the date and time that the infringer's computer was accessing the Internet through the ISP, then the intermediary ISP can review its own subscriber logs to identify the name, addresses, telephone numbers and email addresses of the subscriber.

31. With respect to accused files, CEG sends notices, sometimes referred to as "Digital Millennium Copyright Act notices" or "DMCA notices," to ISPs. Each notice includes the identity of an accused file and the Internet Protocol address of the computer having that file available for download, along with the Timestamp associated with it. In the notice, CEG requests that the ISP forward the notice to the ISP's subscriber associated with the Internet Protocol address. Each notice includes, among other information, an address for the accused infringer to contact CEG to arrange for settlement. In the above-captioned case, the Internet Protocol addresses identified in **Exhibit A** of the above-mentioned Plaintiff's Complaint are those of subscribers who had not settled with CEG. **Exhibit A** lists on a Defendant-by-Defendant basis (one Defendant per row) the IP address associated with each Defendant, the identity of the ISP associated with the IP address, the Timestamp that the infringement by that Defendant was observed by CEG, and the software protocol used by the Defendant in infringing the Plaintiff's Work. The title of the Work, along with its copyright registration number, is set forth on the first page of **Exhibit A**. Note that CEG's System does not monitor all infringers all the time. While the Timestamp indicates the observation of an infringing copy at a computer communicating with the Internet through a particular IP address, it is likely such a computer had an infringing copy of the Work on it at times before and after CEG's System observed the infringement.

32. With respect to Plaintiff's copyrighted motion picture named in the Complaint, CEG performed the steps described in paragraphs 21-31 above. In summary, at least one computer at each of the respective IP addresses listed in **Exhibit A** of the Complaint was used to make an unauthorized digital file copy of at least a substantial portion of Plaintiff's Work and had such at least substantial portion of Plaintiff's Work on it, and, without authorization, was used to make such file available for download by others on a P2P network. As indicated above, all of the infringers identified as "Doe" defendants in the Complaint used BitTorrent software. Further, the hashes associated with the torrent files on the computers having the IP addresses and Timestamps listed in **Exhibit A** are all identical to each other, that is, they all have the same alphanumerical hash. This demonstrates that all the Doe defendants listed in **Exhibit A** joined the same swarm.

33. CEG sent DMCA notices as described above to the ISPs with respect to all the Doe Defendants in the case. None of the ISPs provided the names and addresses of the Doe Defendants to CEG. However, as indicated above, we could determine, from publicly available databases relating to geographic locations of IP addresses, that the Doe Defendants in this case are likely within the state in which this Court is located. (Because of intermediary ISPs and the location of the ISPs technical facilities, these locations cannot be exactly pinpointed from publicly available information.) Without information held by the ISPs, we cannot obtain further information needed to identify the Defendants, including their names, actual addresses, telephone numbers and email addresses.

34. In summary, the Defendants in this case all copied at least a substantial portion of the exact same accused file using the exact same torrent file. Furthermore, because of the nature of BitTorrent software, each Defendant permitted other users to download the accused file from that Defendant's computer. Thus, the Defendants were simultaneously trading (downloading and/or uploading) the exact same file. While Defendants engaged in this downloading and/or uploading of the file, they exposed their globally unique public IP address. With BitTorrent software, one can see the IP address of the various computers that one is connected to, and which are sharing files in cooperation with one's own computer.

35. Continuing the summary, because the Defendants' alleged conduct occurred behind the mask of their respective anonymous IP addresses, neither CEG nor Plaintiff knows the identity of the Doe Defendants, namely the "seeds" and "peers" who utilized BitTorrent to copy, and to allow others to copy, Plaintiff's motion picture. Accordingly, CEG utilized its proprietary file-sharing forensic software to obtain the unique IP addresses that were used by the respective swarm members to distribute Plaintiff's copyrighted work. The software allowed CEG to identify the ISP and unique IP address for each subscriber on the date and at the time of the allegedly infringing activity was observed. Plaintiff therefore identified each Doe Defendant in **Exhibit A** of the Complaint by the unique IP address assigned to the Internet subscriber by the subscriber's ISP at the date and time of the observation.

36. I am informed that before any discovery can be made in civil litigation, a meeting of the parties or the parties' counsel must be held. However, the actual identities of the Doe Defendants are unknown to Plaintiff, and therefore the Complaint cannot be served on any defendant. Without serving the Complaint on any defendant, the pre-discovery meeting cannot be held. Therefore, Plaintiff needs early discovery from the ISPs, and any intermediary ISPs that may be involved, so that the names and addresses of the accused infringers can be obtained by Plaintiff to enable it to enforce its rights in its copyright and prevent continued infringement.

37. ISPs retain their logs for only a limited time. Based on my hands-on experience in working with ISPs, such information is retained for only six months or less on average. Thus, such information must be requested expeditiously and the ISPs must be instructed to retain such information for this litigation.

38. I declare under penalty of perjury that the foregoing is true and correct of my own personal knowledge, except for those matters stated as information and belief, and those matters I believe to be true, and if called upon to testify I can competently do so as set forth above.

Executed this 7th day of April, 2012 in Los Angeles, California.

Jon Nicolini